使用外部syslog伺服器

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/storagegrid-117/monitor/considerations-for-external-syslog-server.html on November 04, 2025. Always check docs.netapp.com for the latest.

目錄

使用外部syslog伺服器 . . . 1
外部syslog伺服器的考量 . . . 1
什麼是外部syslog伺服器？ . . . 1
如何預估外部syslog伺服器的大小 . . . 1
規模估算範例 . . . 3
設定外部syslog伺服器 . . . 4
設定外部伺服器 . . . 5
選取稽核資訊目的地 . . . 10

使用外部**syslog**伺服器

外部**syslog**伺服器的考量

請使用下列準則來預估您所需的外部syslog伺服器大小。

什麼是外部**syslog**伺服器？

外部syslog伺服器是StorageGRID 指不屬於功能區的伺服器、可用來在單一位置收集系統稽核資訊。使用外部syslog伺服器、您可以設定稽核資訊的目的地、以便減少管理節點上的網路流量、並更有效率地管理資訊。您可以傳送至外部syslog伺服器的稽核資訊類型包括：

- 稽核日誌包含正常系統作業期間所產生的稽核訊息
- 安全性相關事件、例如登入和升級至root
- 如果需要開啟支援案例來疑難排解您遇到的問題、可能會要求的應用程式記錄

如何預估外部**syslog**伺服器的大小

一般而言、網格的大小可達到所需的處理量、定義為每秒S3作業量或每秒位元組數。例如、您可能需要網格處理每秒1、000次S3作業、或每秒2、000 MB的物件擷取和擷取作業。您應該根據網格的資料需求來調整外部syslog伺服器的大小。

本節提供一些啟發式公式、可協助您預估外部syslog伺服器需要處理的各種類型的記錄訊息速率和平均大小、以網格的已知或所需效能特性表示（每秒S3作業數）。

在預估公式中使用**S3**作業/秒

如果網格的處理量大小是以每秒位元組數表示、您必須將此規模轉換為每秒S3作業、才能使用估計公式。若要轉換網格處理量、您必須先判斷平均物件大小、以便使用現有稽核記錄和指標（如果有）中的資訊、或是運用您對StorageGRID 使用物件的應用程式所擁有的知識。例如、如果您的網格大小達到每秒2、000 MB的處理量、而且平均物件大小為2 MB、那麼您的網格大小就能處理每秒1、000次S3作業（2、000 MB / 2 MB）。

> ⓘ 下列各節中的外部syslog伺服器規模調整公式提供一般案例預估（而非最糟案例預估）。視組態和工作負載而定、系統記錄訊息或系統記錄資料量的速率可能高於或低於公式所預測的速率。公式只能用作準則。

稽核記錄的估計公式

如果您沒有S3工作負載的相關資訊、而非預期網格支援的每秒S3作業數量、您可以使用下列公式來預估外部syslog伺服器需要處理的稽核記錄數量： 假設您將「稽核層級」設為預設值（所有類別均設為「正常」、但「儲存設備」設為「錯誤」除外）：

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

例如、如果您的網格大小為每秒1、000次S3作業、則外部syslog伺服器的大小應可支援每秒2、000個syslog訊息、而且應能以每秒1.6 MB的速率接收（及儲存）稽核記錄資料。

如果您對工作負載有更深入的瞭解、就有可能進行更精確的評估。在稽核記錄中、最重要的其他變數是S3作業所佔的百分比（相對於（表中使用的4個字元縮寫為稽核記錄欄位名稱）、以及下列S3欄位的平均大小（以位元組為單位）：

程式碼	欄位	說明
SACC	S3租戶帳戶名稱（要求寄件者）	傳送要求之使用者的租戶帳戶名稱。匿名要求為空白。
小型企業	S3租戶帳戶名稱（庫位擁有者）	庫位擁有者的租戶帳戶名稱。用於識別跨帳戶或匿名存取。
S3BK	S3時段	S3儲存區名稱。
S3KY	S3金鑰	S3金鑰名稱、不含儲存區名稱。貯體的作業不包括此欄位。

讓我們使用P來表示S3作業所佔的百分比、其中0≤P≤1（因此、對於100%負載工作負載、P = 1、對於100%取得工作負載、P = 0）。

讓我們用K來表示S3帳戶名稱、S3儲存區和S3金鑰總和的平均大小。假設S3帳戶名稱一律為my-S3帳戶（13位元組）、儲存區具有固定長度的名稱、例如/my/application/bucke-12345（28位元組）、而且物件具有固定長度的金鑰、例如5733a5d7-f069-41ef-8fbd-13247494c69c（36位元組）。然後K值為90（13 + 13 + 28 + 36）。

如果您可以判斷P和K的值、您可以使用下列公式預估外部syslog伺服器需要處理的稽核記錄數量、前提是您將稽核層級設為預設值（所有類別均設為「正常」、儲存除外、 設定為「錯誤」）：

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

例如、如果您的網格大小為每秒1、000次S3作業、則您的工作負載為50%、您的S3帳戶名稱、儲存區名稱、 而且物件名稱平均為90位元組、外部syslog伺服器的大小應可支援每秒1、500則syslog訊息、而且應能以每秒約1 MB的速率接收（及儲存）稽核記錄資料。

非預設稽核層級的估計公式

提供給稽核記錄的公式會假設使用預設的稽核層級設定（所有類別均設定為「正常」、但儲存區設為「錯誤」除外）。對於非預設稽核層級設定、無法使用估算稽核訊息速率和平均大小的詳細公式。不過、下表可用於粗略估計費率； 您可以使用提供給稽核記錄的平均大小公式、但請注意、這可能會導致預估過度、因為「額外」稽核訊息平均比預設稽核訊息小。

條件	公式
複寫：稽核層級全部設為「偵錯」或「正常」	稽核記錄率= 8 x S3作業率
銷毀編碼：稽核層級全部設為「除錯」或「正常」	使用與預設設定相同的公式

安全性事件的估計公式

安全事件與 S3 作業無關、通常會產生可忽略的記錄和資料量。因此、我們不會提供任何預估公式。

應用程式記錄的估計公式

如果您沒有S3工作負載的相關資訊、而不是預期網格支援的每秒S3作業數量、您可以使用下列公式來預估外部syslog伺服器需要處理的應用程式記錄數量：

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

例如、如果您的網格大小為每秒1、000次S3作業、則外部syslog伺服器的大小應可支援每秒3、300個應用程式記錄、並能以每秒1.2 MB的速率接收（及儲存）應用程式記錄資料。

如果您對工作負載有更深入的瞭解、就有可能進行更精確的評估。對於應用程式記錄、最重要的其他變數是資料保護策略（複寫與銷毀編碼）、所放置S3作業的百分比（與獲得/其他）、以及下列S3欄位的平均大小（以位元組為單位）（表中使用的4個字元縮寫為稽核記錄欄位名稱）：

程式碼	欄位	說明
SACC	S3租戶帳戶名稱（要求寄件者）	傳送要求之使用者的租戶帳戶名稱。匿名要求為空白。
小型企業	S3租戶帳戶名稱（庫位擁有者）	庫位擁有者的租戶帳戶名稱。用於識別跨帳戶或匿名存取。
S3BK	S3時段	S3儲存區名稱。
S3KY	S3金鑰	S3金鑰名稱、不含儲存區名稱。貯體的作業不包括此欄位。

規模估算範例

本節說明如何使用下列資料保護方法來使用網格的估計公式範例：

- 複寫
- 銷毀編碼

如果您使用複寫來保護資料

讓P代表S3作業所放置的百分比、其中0≤P≤1（因此、對於100%投入工作負載、P = 1、對於100%取得工作負載、P = 0）。

讓K代表S3帳戶名稱、S3儲存區和S3金鑰總和的平均大小。假設S3帳戶名稱一律為my-S3帳戶（13位元組）、儲存區具有固定長度的名稱、例如/my/application/bucke-12345（28位元組）、而且物件具有固定長度的金鑰、例如5733a5d7-f069-41ef-8fbd-13247494c69c（36位元組）。然後K值為90（13 + 13 + 28 + 36）。

如果您可以判斷P和K的值、您可以預估外部syslog伺服器必須使用下列公式才能處理的應用程式記錄數量。

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

例如、如果您的網格大小為每秒1、000次S3作業、工作負載為50%、S3帳戶名稱、儲存區名稱及物件名稱平均為90個位元組、則外部syslog伺服器的大小應可支援每秒1800個應用程式記錄、 並以每秒0.5 MB的速率接收（通常是儲存）應用程式資料。

如果您使用銷毀編碼來保護資料

讓P代表S3作業所放置的百分比、其中0≤P≤1（因此、對於100%投入工作負載、P = 1、對於100%取得工作負載、P = 0）。

讓K代表S3帳戶名稱、S3儲存區和S3金鑰總和的平均大小。假設S3帳戶名稱一律為my-S3帳戶（13位元組）、儲存區具有固定長度的名稱、例如/my/application/bucke-12345（28位元組）、而且物件具有固定長度的金鑰、例如5733a5d7-f069-41ef-8fbd-13247494c69c（36位元組）。然後K值為90（13 + 13 + 28 + 36）。

如果您可以判斷P和K的值、您可以預估外部syslog伺服器必須使用下列公式才能處理的應用程式記錄數量。

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

例如、如果您的網格大小為每秒1、000次S3作業、則您的工作負載為50%、您的S3帳戶名稱、儲存區名稱、 物件名稱平均為90個位元組、您的外部syslog伺服器的大小應可支援每秒2、250個應用程式記錄、且應能以每秒0.6 MB的速率接收（通常是儲存）應用程式資料。

如需設定稽核訊息層級和外部 Syslog 伺服器的詳細資訊、請參閱下列內容：

- "設定外部syslog伺服器"
- "設定稽核訊息和記錄目的地"

設定外部syslog伺服器

如果您想要將稽核記錄、應用程式記錄和安全性事件記錄儲存到網格以外的位置、請使用此程序來設定外部syslog伺服器。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您具有「維護」或「根」存取權限。
- 您有一部具備接收及儲存記錄檔容量的syslog伺服器。如需詳細資訊、請參閱 "外部syslog伺服器的考量"。
- 如果您計畫使用TLS或RELP/TLS、則您擁有正確的伺服器和用戶端認證。

關於這項工作

如果您想要傳送稽核資訊到外部syslog伺服器、則必須先設定外部伺服器。

將稽核資訊傳送至外部syslog伺服器、可讓您：

- 更有效率地收集和管理稽核資訊、例如稽核訊息、應用程式記錄和安全性事件
- 減少管理節點上的網路流量、因為稽核資訊會直接從不同的儲存節點傳輸到外部syslog伺服器、而不需要經過管理節點

> 當記錄傳送至外部syslog伺服器時、訊息結尾處會截短大於8192位元組的單一記錄、以符合外部syslog伺服器實作的一般限制。

> 為了在外部syslog伺服器發生故障時、將完整資料還原的選項最大化、每個節點上最多可維護20GB的稽核記錄本機記錄（localremote.log）。

> 如果此程序中可用的組態選項不夠靈活、無法滿足您的需求、則可使用私有 API 套用其他組態選項 `audit-destinations` 端點。例如、不同節點群組可以使用不同的syslog伺服器。

設定外部伺服器

存取精靈

若要開始、請存取「設定外部 Syslog 伺服器」精靈。

步驟

1. 選擇*組態*>*監控*>*稽核與系統記錄伺服器*。
2. 從「稽核與系統記錄伺服器」頁面、選取*「設定外部系統記錄伺服器*」。如果您先前已設定外部syslog伺服器、請選取*編輯外部syslog伺服器*。

   此時將顯示 Configure external Syslog server （配置外部系統日誌服務器）

輸入**syslog**資訊

您必須提供 StorageGRID 存取外部 Syslog 伺服器所需的資訊。

步驟

1. 在嚮導的 * 輸入系統日誌 info* 步驟中，在 * 主機 * 字段中輸入外部系統日誌服務器的有效完全限定域名或 IPv4 或 IPv6 地址。
2. 輸入外部syslog伺服器上的目的地連接埠（必須是介於1和6555之間的整數）。預設連接埠為514。
3. 選取用於傳送稽核資訊至外部syslog伺服器的傳輸協定。

   建議使用 **TLS** 或 **RELP/TLS** 。您必須上傳伺服器憑證、才能使用上述任一選項。使用憑證有助於保護網格與外部syslog伺服器之間的連線。如需詳細資訊、請參閱 "管理安全性憑證"。

   所有的傳輸協定選項都需要外部syslog伺服器的支援和組態。您必須選擇與外部syslog伺服器相容的選項。

可靠的事件記錄傳輸協定（RELP）可延伸系統記錄傳輸協定的功能、以提供可靠的事件訊息傳輸。如果您的外部syslog伺服器必須重新啟動、使用RELP有助於防止稽核資訊遺失。

4. 選擇*繼續*。
5. [[attach認證]如果您選取* TLS*或* RELP/TLS*、請上傳下列認證：
   - 伺服器**CA**憑證：一或多個用於驗證外部系統記錄伺服器的信任CA憑證（以PEEM編碼）。如果省略、則會使用預設的Grid CA憑證。您在這裡上傳的檔案可能是CA套裝組合。
   - 用戶端憑證：用於驗證外部syslog伺服器的用戶端憑證（以PEEM編碼）。
   - 用戶端私密金鑰：用戶端憑證的私密金鑰（以PEEM編碼）。

     如果您使用用戶端憑證、也必須使用用戶端私密金鑰。如果您提供加密的私密金鑰、也必須提供密碼。使用加密的私密金鑰並無顯著的安全效益、因為必須儲存金鑰和通關密碼；建議使用未加密的私密金鑰（若有）、以簡化操作。

     i. 選取*瀏覽*以取得您要使用的憑證或金鑰。
     ii. 選取憑證檔案或金鑰檔。
     iii. 選取*「Open*（開啟*）」上傳檔案。

     憑證或金鑰檔名稱旁會出現綠色勾號、通知您已成功上傳。
6. 選擇*繼續*。

管理系統記錄內容

您可以選取要傳送至外部 Syslog 伺服器的資訊。

步驟

1. 針對精靈的 * 管理系統記錄內容 * 步驟、選取您要傳送至外部系統記錄伺服器的每種稽核資訊類型。
   - * 傳送稽核記錄 * ：傳送 StorageGRID 事件和系統活動
   - * 傳送安全性事件 * ：傳送安全性事件，例如未獲授權的使用者嘗試登入或使用者以 root 身分登入
   - * 傳送應用程式記錄 * ：傳送有助於疑難排解的記錄檔、包括：
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` （僅限管理節點）
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`
2. 使用下拉式功能表、為您要傳送的稽核資訊類別選取嚴重性和設施（訊息類型）。

   如果您選擇* Passthsthsthation*作為嚴重性和設施、則傳送至遠端syslog伺服器的資訊將會收到與登入本機節點時相同的嚴重性和設施。設定設施和嚴重性可協助您以可自訂的方式彙總記錄、以便更輕鬆地進行分

析。

如需 StorageGRID 軟體記錄的詳細資訊、請參閱 "軟體記錄StorageGRID"。

a. 對於*嚴重性*、如果您希望傳送至外部系統記錄的每則訊息嚴重性值與本機系統記錄中的嚴重性值相同、請選取* Passthsth*。

   對於稽核記錄、如果您選取 * Passthrough * 、嚴重性為「 info 」。

   對於安全性事件、如果您選取 * Passthrough * 、嚴重性值會由節點上的 Linux 發佈版本產生。

   對於應用程式記錄、如果您選取* Passthsthon*、則「資訊」與「通知」之間的嚴重性會因問題而異。例如、新增 NTP 伺服器並設定 HA 群組會提供「 info 」的值、而刻意停止 SSM 或 RSM 服務則會提供「 notice 」的值。

b. 如果您不想使用傳遞值、請選取介於 0 和 7 之間的嚴重性值。

   選取的值將套用至此類型的所有訊息。當您選擇以固定值覆寫嚴重性時、會遺失不同嚴重性的相關資訊。

嚴重性	說明
0	緊急：系統無法使用
1.	警示：必須立即採取行動
2.	關鍵：關鍵條件
3.	錯誤：錯誤情況
4.	警告：警告條件
5.	注意：正常但重要的情況
6.	資訊：資訊訊息
7.	偵錯：偵錯層級的訊息

c. 對於* Facility 、如果您希望傳送至外部**syslog**的每則訊息具有與本機**syslog**相同的設施值、請選取Passthsth*。

   對於稽核記錄、如果您選取 * Passthrough * 、則傳送至外部 Syslog 伺服器的設備為「 local7 」。

   對於安全事件、如果您選取* Passthsth*、則設施值會由節點上的Linux發佈套件產生。

   對於應用程式記錄、如果您選取* Passthsthsth*、則傳送至外部syslog伺服器的應用程式記錄檔具有下列設施值：

應用程式記錄	傳遞值
bycast.log	使用者或精靈
bycast-err.log	使用者、精靈、local3或local4
jaeger.log	local2
nms.log	local3
prometheus.log	本地4
raft.log	本地5.
hagroups.log	local6.

d. 如果您不想使用傳遞值、請選取介於 0 和 23 之間的醫事機構值。

選取的值將套用至此類型的所有訊息。當您選擇以固定值覆寫設施時、將會遺失有關不同設施的資訊。

設施	說明
0	KERN（核心訊息）
1.	使用者（使用者層級訊息）
2.	郵件
3.	精靈（系統精靈）
4.	驗證（安全性/授權訊息）
5.	系統記錄（系統記錄所產生的訊息）
6.	LPR（線路印表機子系統）
7.	新聞（網路新聞子系統）
8.	uucp
9.	cron（時鐘精靈）
10.	安全性（安全性/授權訊息）

設施	說明
11.	FTP
12.	NTP
13.	記錄稽核（記錄稽核）
14	記錄警示（記錄警示）
15	時鐘（時鐘精靈）
16	local0
17	local1
18	local2
19	local3
20	本地4
21	本地5.
22	local6.
23	本地化7.

3. 選擇*繼續*。

傳送測試訊息

開始使用外部syslog伺服器之前、您應該要求網格中的所有節點都將測試訊息傳送至外部syslog伺服器。您應該使用這些測試訊息來協助驗證整個記錄收集基礎架構、然後再將資料傳送至外部syslog伺服器。

請勿使用外部 Syslog 伺服器組態、除非您確認外部 Syslog 伺服器收到來自網格中每個節點的測試訊息、且訊息已如預期般處理。

步驟

1. 如果您不想傳送測試訊息、因為您確定已正確設定外部 Syslog 伺服器、而且可以從網格中的所有節點接收稽核資訊、請選取 * 略過並完成 * 。

   此時會出現綠色橫幅、表示您的組態已成功儲存。

2. 否則、請選取 * 傳送測試訊息 * （建議）。

測試結果會持續顯示在頁面上、直到您停止測試為止。測試進行中時、您的稽核訊息會繼續傳送至先前設定的目的地。

3. 如果您收到任何錯誤、請更正錯誤、然後再次選取*傳送測試訊息*。

   請參閱 "排除外部syslog伺服器的故障" 協助您解決任何錯誤。

4. 請等到看到綠色橫幅、表示所有節點都已通過測試。
5. 請檢查您的syslog伺服器、確定是否收到測試訊息、並按照預期處理。

   如果您使用的是udp、請檢查整個記錄收集基礎架構。此udp傳輸協定不允許像其他傳輸協定一樣嚴格的錯誤偵測。

6. 選擇*停止並結束*。

   您將返回到* Audit和syslog server*頁面。此時會出現綠色橫幅、通知您已成功儲存系統記錄伺服器組態。

   除非您選取包含外部syslog伺服器的目的地、否則您的「不稽核資訊」不會傳送到外部syslog伺服器。StorageGRID

選取稽核資訊目的地

您可以指定安全性事件記錄、應用程式記錄和稽核訊息記錄的傳送位置。

如需 StorageGRID 軟體記錄的詳細資訊、請參閱 "軟體記錄StorageGRID"。

步驟

1. 在「稽核與syslog伺服器」頁面上、從列出的選項中選取稽核資訊的目的地：

選項	說明
預設（管理節點/本機節點）	稽核訊息會傳送至稽核記錄 (`audit.log`）在管理節點上、安全性事件記錄和應用程式記錄會儲存在產生它們的節點上（也稱為「本機節點」）。
外部syslog伺服器	稽核資訊會傳送至外部syslog伺服器、並儲存在本機節點上。傳送的資訊類型取決於您設定外部syslog伺服器的方式。只有在設定外部syslog伺服器之後、才會啟用此選項。
管理節點和外部syslog伺服器	稽核訊息會傳送至稽核記錄 (`audit.log`）、稽核資訊會傳送至外部Syslog 伺服器、並儲存在本機節點上。傳送的資訊類型取決於您設定外部syslog伺服器的方式。只有在設定外部syslog伺服器之後、才會啟用此選項。

選項	說明
僅限本機節點	不會將稽核資訊傳送至管理節點或遠端syslog伺服器。稽核資訊只會儲存在產生該資訊的節點上。 附註：StorageGRID 此功能會定期移除這些本機記錄、以釋出空間。當節點的記錄檔達到1 GB時、會儲存現有檔案、並啟動新的記錄檔。記錄檔的旋轉限制為21個檔案。建立22版記錄檔時、會刪除最舊的記錄檔。每個節點平均儲存約20 GB的記錄資料。

每個本機節點上產生的稽核資訊都儲存在中 `/var/local/log/localaudit.log`

2. 選擇*保存*。然後，選擇 **OK** 以接受對日誌目的地的更改。
3. 如果您選擇*外部系統記錄伺服器*或*管理節點和外部系統記錄伺服器*作為稽核資訊的目的地、則會出現額外的警告。檢閱警告文字。

   您必須確認外部syslog伺服器可以接收測試StorageGRID 用的資訊。

4. 選取 * 確定 * 以確認您要變更稽核資訊的目的地。

   此時會出現綠色橫幅、通知您稽核組態已成功儲存。

   新記錄會傳送至您選取的目的地。現有記錄仍會保留在目前位置。

相關資訊

"稽核訊息總覽"

"設定稽核訊息和記錄目的地"

"系統稽核訊息"

"物件儲存稽核訊息"

"管理稽核訊息"

"用戶端讀取稽核訊息"

"管理StorageGRID"

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。